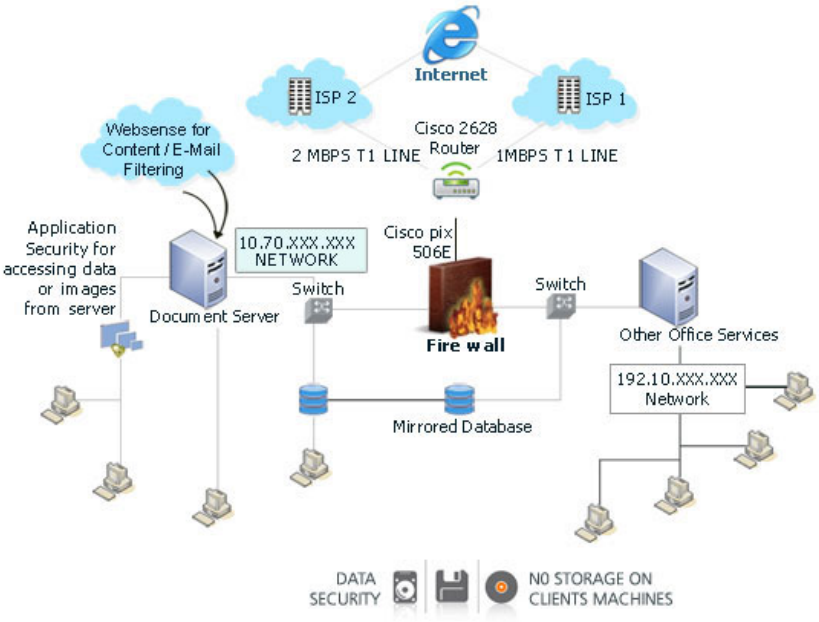
Wipe out the risk of attack inside encrypted data

For a business that is concerned about security, the potential 'hidden' risks hidden within SSL are encrypted, which is not to be missed.

***TipsMake.com* - For an enterprise interested in security issues, the potential 'hidden' risks hidden within SSL are encrypted which is not to be missed. If SSL is used for no special purpose, the problem can be solved more simply by avoiding or preventing the use of SSL. However, the truth is different. SSL is used to provide much-needed security measures in a wide range of applications.**



Today, most businesses have security applications that provide protection against attacks targeted at business computing. In addition, these applications prevent the loss of important business data. These applications work by attaching network traffic to an attack identification identity signature or monitoring application status as a tool to detect ambiguous operations.

Another security way to help ensure these security applications do not detect the risk of attack or data loss is to prevent signature bindings and track the current page when operating; The easiest way to do this is to encrypt network traffic.

If network encryption is only used for a small amount of network traffic, then the fact that the attack risks can hide inside encrypted traffic is not a big problem. However, Secure Sockets Layer (SSL) - the encryption protocol for information - is widely used to protect network traffic, and the number of SSL traffic has increased

significantly in recent years.

HTTPS, simply the protocol that runs on SSL, is the basic interface for most Web 2.0 and cloud applications and is also the default interface for widely used applications such as Gmail, Yahoo mail and Google.

An enterprise network can find today that about 20 to 80% of the traffic on the network is SSL encrypted, and that number is increasing with time.

Double-edged sword

All SSL traffic is encrypted and, unfortunately, a similar tool being used to encrypt traffic prevents attacks is also the key to opening attacks. Because SSL helps data transmission be secure and encrypted, attackers can also use this technology effectively to hide their attack malicious code.

The security structure used by businesses today to protect data does not have the ability to detect content inside encrypted data.

For example, for most businesses, having more than 50% of the traffic to and from the network must go through the security structure. The attacks targeted at enterprise web servers will not be blocked by Intrusion Prevention System (IPS) - a solution against illegal intrusion; Malware from Internet sites that use HTTPS protocol will hurt businesses' desktop computers; and mail sent on webmail via HTTPS runs the risk of important information leakage, despite the presence of Data Loss Prevention (DLP) data loss system.

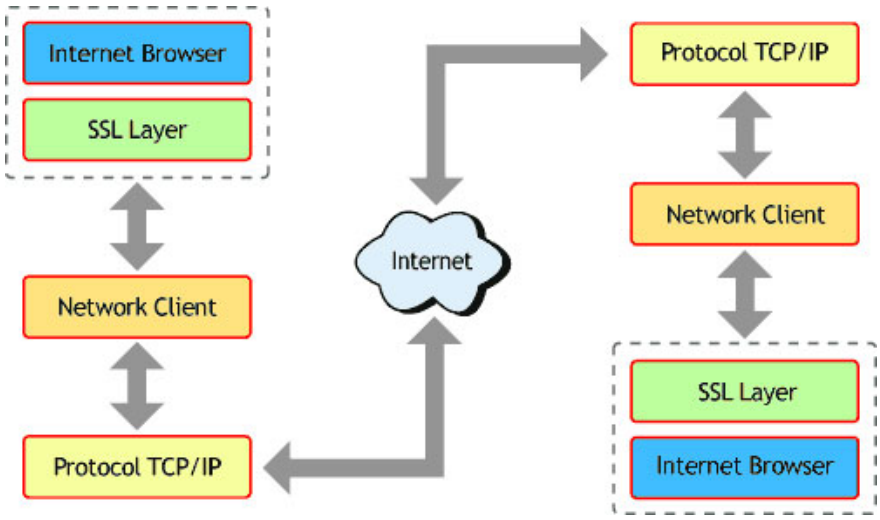
For a business concerned about security, focusing on the risk posed by malicious code or virus hidden in encrypted SSL traffic is not negligible.

If SSL is used for no special purpose, the problem can be solved more simply by avoiding or preventing the use of SSL. However, the truth is different. SSL is used to provide much-needed security measures in a wide range of applications.

For example, allowing webmail not to use SSL means that corporate email can spread over the public network and attackers can easily access it. In addition, using Google applications without SSL support will "expose" your important data to anyone who can access them when they use the Internet.

With the rise of online shopping, e-commerce traffic without 'patronage' of SSL seems hard to succeed, because most users know that a website is trustworthy when the browser of they display the lock icon, indicating that SSL is being used.

The problem with this problem is how to use encrypted traffic but it can still prevent them from making security applications useless. There are several methods to help solve this problem. Each solution provides a different way to turn encrypted content of a network to 'shake hands' with security applications but still keep the point-to-point encryption between the client and server, in order to ensure the best security. The methods differ in their impact on application performance, network configuration complexity and client customization requirements.



Fully authorized

One method is to leverage the fully authorized device, complete the end and then re-restart the structure of an application. This method requires only authorized proxy applications to use SSL. As soon as the authorized device fully supports SSL endpoints and re-start and application layer, then it will access unencrypted content.

While the content is not encrypted, the authorized device can fully perform security checks on the data or it can send a copy of the unencrypted data to a secure application. Let this app do the search.

Authorized devices also often require that the client need to be configured to know the device and have direct connection to the usage of the device-related applications. However, this requires permanent management. This also means that a client can be configured to not take advantage of the device.

SSL Proxy is clear

Another alternative is to use a transparent, transparent SSL Proxy in connection with existing security applications that are deployed in the local network. A SSL Proxy obviously does not need to understand or be able to handle application layer protocols and this Proxy is optimized for limiting and reorganizing the SSL protocol layer.

In addition, this Proxy is deployed at a point in the network, where all the traffic of commonly used applications will be displayed. It will help detect all SSL traffic, thoroughly examine the packets, and be able to decrypt and re-encrypt the traffic so that you can access encrypted traffic. These traffic is then packaged into a 'generated' TCP stream and sent to one or more security applications available in the network.

Once security applications receive unencrypted traffic, they will do their job and detect if there is any threat or data leak. If the security application is a filtering device, such as IPS, it will remove malicious traffic, and SSL Proxy will rediscover the traffic and remove the corresponding SSL stream.

If the security application is IDS or a Network Forensics device, the application will generate reports of detected threats in unencrypted traffic.

Because traffic does not need to be sent explicitly to Proxy, these Proxies do not require client configuration. In addition, since they do not end and rearrange application-layer protocols, they do not need delay time and can

operate at high speeds.

Because proxies do not require the use of security applications on an enterprise network, they do not make it difficult to operate and they do not require changes in the network or client configuration.

As the amount of encrypted data traffic continues to increase, businesses need to find ways to make sure that the security applications installed do not become useless by SSL traffic. Proxies are obviously the best solution in facing the risks from malicious code hidden inside SSL traffic.